UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/817,124	04/02/2004	Glenn A. Morten	08223/1200330-US2	1508

7278 7590 06/10/2008

DARBY & DARBY P.C.
P.O. BOX 770
Church Street Station
New York, NY 10008-0770

EXAMINER	
JOHNSON, CARLTON	
ART UNIT	PAPER NUMBER
2136	
MAIL DATE	DELIVERY MODE
06/10/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/817,124	MORTEN ET AL.	
	Examiner	Art Unit	
	CARLTON V. JOHNSON	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *3-12-2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114.
Applicant's submission filed on 3/12/2008 has been entered.

2. This action is responding to application papers filed on **4-2-2004**. Claims **1 - 20** are pending. Claims **1, 12, 18, 20** have been amended. Claims **1, 12, 18, 20** are independent.

Response to Arguments

3. Applicant's arguments filed 3/12/2008 have been fully considered but they are not persuasive.

3.1 Applicant argues that the referenced prior art does not disclose, (1) receive content; (2) decrypt content; (3) watermark content; and (4) encrypt content. (see Remarks Pages 8-9)

Surely applicant is not claiming encryption and decryption of media content as its claimed invention. These are well known in the art procedures that are completed by the claimed invention during the processing of media content. Benaloh discloses

encryption and decryption of media content as an additional security mechanism. (see Benaloh col. 1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content; col. 2, lines 8-10: content decrypted; col. 10, lines 6-10: encrypt contents)

Surely applicant is not claiming the media content distribution chain and the usage of first (second, third, ..., or etc) market participants. Resellers for media content is no different than the original content owner who watermarks his/or her media content to uniquely identify the content as belonging to the media content owner. Cooper discloses a media content distributor. The media content is watermarked before it is transferred to a user as per claimed invention. (see Cooper paragraph [0037], lines 1-3; paragraph [0019], lines 5-9; paragraph [0198], lines 8-19: content is transferred to a user; content distributor)

Applicant's invention appears to be the ability to watermark content with a watermark that is uniquely identifiable to a specific individual or entity and the placement of multiple watermarks if necessary onto a piece of media content. The entity in this case is the market participant or downstream media content reseller. Cooper discloses that a watermark is placed upon content that uniquely identifies the entity that watermarks the content. (see Cooper paragraph [0196], lines 1-7: unique identifier for media content and where it came from (distributor))

Cooper discloses the concept and capability of a content distributor. And, Cooper discloses the ability to watermark content, encrypt media content and download the media content to a user. These actions are the same actions outlined in claim 1. Take

(received) media content, place a unique watermark upon content, encrypt, and distribute the encrypted content. (see Cooper paragraph [0198], lines 8-19: watermark and encrypt content) And, Cooper discloses the placement of multiple watermarks onto media content. (see Cooper paragraph [0249], lines 1-15: multiple watermarks)

3.2 Applicant argues that the referenced prior art does not disclose, watermark uniquely identifies content. (see Remarks Pages 8-11)

In the claimed invention the content is watermarked with an identifier that uniquely identifies or is associated with an entity. The entity in this case is the market participant or reseller or distributor of media content. This appears to be the principal and alleged novelty of the claimed invention. There is no indication that this must not be accomplished by using a certificate authority or any other certificate related mechanism. In any event, Cooper prior art discloses an ability to place a watermark onto media content that uniquely identifies an entity. (see Cooper paragraph [0196], lines 1-7: watermark, unique identification where content came from)

Applicant states that the Cooper prior art discloses that the content is watermarked and encrypted after placement of watermark before transmission to user. These are the functions of a content distributor and Cooper is a content distributor and not a user. (see Cooper paragraph [0196], lines 1-7: unique identifier for media content and where it came from (distributor); paragraph [0198], lines 8-19; encrypt content, customer ID may also be added as an additional watermark)

3.3 Applicant argues that the referenced prior art does not disclose, placement of multiple watermarks. (see Remarks Page 11)

Cooper prior art discloses the capability for multiple watermarks to be place onto media content and encryption of the media content after watermark(s) placement. (see Cooper paragraph [0249], lines 1-15: multiple watermarks placed onto media content)

3.4 Benaloh prior art discloses the encryption and decryption of media content. Benaloh and Cooper prior art disclose a watermark mechanism for the placement of a watermark onto media content that uniquely identifies an entity such as a media content distributor. And, Benaloh and Cooper discloses the ability to place multiple watermarks onto media content.

After an additional analysis of the applicant's invention, remarks, and a search of the available prior art, it was determined that the current set of prior art consisting of Benaloh (7,065,216) and Cooper (20010051996) discloses applicant's invention.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims **1 - 20** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Benaloh et al.** (US Patent No. **7,065,216)** in view of **Cooper et al.** (US PGPUB No.

20010051996) .

With Regards to Claim 1, Benaloh discloses a method for tracing content in a highly distributed system, comprising:

a) receiving content associated with a content owner from a first entity in the highly distributed system; (see Benaloh col. 1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content)

b) decrypting the received content by a second entity that received the content from the first entity; (see Benaloh col. 2, lines 8-10: content decrypted)

c) determining a self-identifier that uniquely identifies an entity decrypting the content; (see Benaloh col. 6, lines 25-27: serial number, identifier for content player)

d) modifying the decrypted content by the second entity by embedding at least one of a fingerprint or a watermark into the decrypted content, wherein the fingerprint or watermark is generated, in part, from the self-identifier; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

e) encrypting the modified content by the second entity; (see Benaloh col. 10, lines 6-10: encrypt contents)

f) wrapping the encrypted modified content together with the self-identifier using an access key; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

Benaloh discloses a highly distributed system for content delivery. (see Benaloh col.

1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content) Benaloh does not specifically disclose providing a set of information to the content owner, wherein the set of information enables the content owner to trace the content in the highly distributed system.

However, Cooper discloses:

g) providing a set of information to the content owner, wherein the set of information enables the content owner to trace the content in the highly distributed system. (see Cooper paragraph [0071], lines 1-4; paragraph [0298], lines 1-3: report unauthorized content usage)

It would have been obvious to one of ordinary skill in the art to modify Benaloh to provide a set of information to the content owner, wherein the set of information enables the content owner to trace the content in the highly distributed system as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13: "*... Therefore, there is a need in the electronic media content distribution field to be able to mark content files with an authenticated digital signature that uniquely identifies the person who is the source, to be able to monitor the files if they are transferred to others, and to have these capabilities while imposing minimal burden and inconvenience on the consumer. ...* ")

With Regards to Claims 2, 8, Benaloh discloses the method of claims 1, 7, wherein

decrypting the received content further comprises:

a) obtaining a different access key out-of-band, wherein the different access key is uniquely associated with the entity decrypting the content and a sender of the content; (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14; col. 6, lines19-23: receive content (access) key (network, other)) and

b) employing the different access key to unwrap the received content before decrypting the received content. (see Benaloh col. 10, lines 16-19: decrypt content using access key)

With Regards to Claim 3, Benaloh discloses the method of claim 1, wherein the fingerprint or watermark is further generated based on another self-identifier that uniquely identifies a downstream market recipient of the content. (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint; col. 6, lines 25-27: serial number, identifier for content player (downstream market recipient))—

With Regards to Claim 4, Benaloh discloses the method of claim 1, wherein the self-identifier associated with the entity decrypting the content. (see Benaloh col. 6, lines 25-27: serial number, identifier for content player to decrypt content) Benaloh does not specifically disclose the capability to digitally sign with an encryption key. However, Cooper discloses wherein the self-identifier is digitally signed content by an encryption key. (see Cooper paragraph [019], lines 1-2: content distribution; paragraph [0043], lines 1-5: digitally sign content; paragraph [0019], lines 5-9: watermark-fingerprint

techniques)

It would have been obvious to one of ordinary skill in the art to modify Benaloh to digitally sign with an encryption key as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

With Regards to Claim 5, Benaloh discloses the method of claim 1, wherein the self-identifier further comprises at least one of a serial number, and a time stamp indicating approximately when the content is decrypted. (see Benaloh col. 6, lines 25-27: serial number, identify content player)

With Regards to Claim 6, Benaloh discloses the method of claim 1, wherein the set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the entity decrypting the content. (see Benaloh col. 2, lines 36-39: traceability information)

With Regards to Claim 7, Benaloh discloses the method of claim 1, further comprising:

a) providing the wrapped encrypted modified content and self-identifier to a downstream market recipient; (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to end user, downstream market recipient)
b) decrypting by the downstream market recipient, the received modified content;

(see Benaloh col. 2, lines 8-10: content decrypted)

c) further modifying the decrypted modified content by embedding another fingerprint or watermark into the modified content, wherein the other fingerprint or watermark is generated in part from another self-identifier that uniquely identifies the downstream market recipient that decrypts the modified content; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

d) encrypting the further modified content; (see Benaloh col. 10, lines 6-10: encrypt contents) and

And, Cooper discloses:

e) wrapping the encrypted further modified content together with the self-identifier that uniquely identifies the entity decrypting the content and the self-identifier that uniquely identifies the downstream market recipient. (see Cooper paragraph [0198], lines 8-19: watermark, encrypt, unique identifier; may add customer ID (downstream identifier))

It would have been obvious to one of ordinary skill in the art to modify Benaloh to digitally sign with an encryption key as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

With Regards to Claim 9, Benaloh discloses the method of claim 1, wherein

generating encrypted content. (see Benaloh col. 10, lines 6-10: encrypting content) Benaloh does not specifically disclose wrapping the encrypted content further comprises digitally signing the encrypted content. However, Cooper discloses wherein wrapping the encrypted content further comprises digitally signing the encrypted content. (see Cooper paragraph [019], lines 1-2: content distribution; paragraph [0043], lines 1-5: digitally sign content; paragraph [0019], lines 5-9: watermark-fingerprint techniques)

It would have been obvious to one of ordinary skill in the art to modify Benaloh to wrap the encrypted content further comprising digitally signing the encrypted content as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

With Regards to Claim 10, Benaloh discloses the method of claim 1, wherein the access key employs a public key infrastructure. (see Benaloh col. 6, lines 13-18; col. 10, lines 6-10: public/private key pair techniques)

With Regards to Claim 11, Benaloh discloses the method of claim 1, wherein the content is at least one of a subscription television, movies, interactive video games, video conferencing, audio, still images, text, graphics. (see Benaloh col. 7, lines 1-5: content, a movie)

With Regards to Claim 12, Benaloh discloses a security device for tracing content in a highly distributed system, comprising:

a) a receiver configured to receive and decrypt encrypted content associated with a content owner; (see Benaloh col. 1, lines 63-66: content received (provided); col. 12, lines 10-14: network (distributed) access to content)

b) a fingerprinter-watermarker configured to perform actions including: determining a self-identifier that uniquely identifies the security device decrypting the content; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

c) generating a fingerprint, in part, from the self-identifier; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

d) watermarking the content by the security device employing the fingerprint; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

Benaloh does not specifically disclose a forensics interface configured to send information associated with the watermarked content to the content owner. However, Cooper discloses:

e) a forensics interface configured to send information associated with the watermarked content to the content owner. (see Cooper paragraph [0071], lines 1-4; paragraph [0298], lines 1-3: report unauthorized content usage)

It would have been obvious to one of ordinary skill in the art to modify Benaloh

for a forensics interface configured to send information associated with the watermarked content to the content owner as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

With Regards to Claim 13, Benaloh discloses the security device of claim 12, further comprising:

a) a key wrap, coupled to the fingerprinter-watermarker(see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint),

that is configured to perform actions, including:

b) receiving an access key associated with the recipient of the content; (see Benaloh col. 7, lines 1-5: receive content (access key)) and

c) wrapping the content together with the self identifier employing the access key. (see Benaloh col. 10, lines 6-10: encrypt content and security information using content (access) key)

With Regards to Claim 14, Benaloh discloses the security device of claim 13, wherein the access key is received employing an out-of-band mechanism. (see Benaloh col. 10, lines 20-28; col. 12, lines 12-14; col. 6, lines19-23: receive content (access) key, (network, other))

With Regards to Claim 15, Benaloh discloses the security device of claim 12, wherein the recipient is at least one of an aggregator, a service operator, and a user. (see Benaloh col. 4, line 66 - col. 5, line 5: content provider(s), aggregator)

With Regards to Claim 16, Benaloh discloses the security device of claim 12, wherein the second set of information further comprises at least one of traceability information, a time stamp, an identifier, and registration information associated with at least one of the content and the recipient of the content. (see Benaloh col. 2, lines 36-39: traceability information)

With Regards to Claim 17, Benaloh discloses the security device of claim 12, further comprising:

b) a fingerprinted-watermarked content data store configured to store encrypted content. (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

Benaloh does not specifically disclose a data store configured to store decrypted content.

However, Cooper discloses:

a) a data store configured to store decrypted content; (see Cooper paragraph [019], lines 1-2: content distribution; paragraph [0018], lines 12-15; paragraph [0062], lines 2-6: database; paragraph [0019], lines 5-9: watermark-fingerprint techniques)

It would have been obvious to one of ordinary skill in the art to modify Benaloh for a data store configured to store decrypted content as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

With Regards to Claim 18, Benaloh discloses a network device for managing content in a highly distributed system, comprising:

a) a transceiver that is arranged to receive and to send content to another network device; (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to user (network, medium)) and

at least one processor that is configured to execute program code to perform actions, including:

b) receiving a first wrapper of content from a first market participant sent to a second market participant that is associated with the network device, the wrapper including encrypted content, a first identifier that uniquely identifies the first market participant, and a content key, wherein the encrypted content, content key, and unique first identifier are together encrypted into the first wrapper using an access key associated with the network device; (see Benaloh col. 6, lines 25-27: serial number, identifier for content player; col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

c) decrypting the first wrapper using the access key at the network device of the second market participant; decrypting the encrypted content using the decrypted content key at the network device of the second market participant; (see Benaloh col. 2, lines 8-10: content decrypted)

d) generating at least one of a fingerprint or a watermark that uniquely identifies the second market participant; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

e) marking at the network device of the second market participant the decrypted content by embedding the fingerprint or watermark into the decrypted content; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

f) encrypting at the network device of the second market participant the marked content using the content key; (see Benaloh col. 10, lines 6-10: encrypt contents)

g) generating a second wrapper that wraps together the content key, the encrypted marked content, the first unique identifier, and a second unique identifier that uniquely identifies the second market participant, using an access key associated with a third market participant; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint) and

i) transmitting the second wrapper to the third market participant. (see Benaloh col. 10, lines 20-28; col. 12, lines 10-14: transfer encrypted content to user (network, medium))

Benaloh does not specifically disclose providing the information concerning the decrypted content to the content owner.

However, Cooper discloses:

d) providing the information concerning the decrypted content to the content owner. (see Cooper paragraph [0071], lines 1-4; paragraph [0298], lines 1-3: report unauthorized content usage)

It would have been obvious to one of ordinary skill in the art to modify Benaloh for providing the information concerning the decrypted content to the content owner as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

With Regards to Claim 19, Benaloh discloses the network device of claim 18, wherein the second unique identifier further includes a time stamp that further indicates when the second wrapper is created. (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint)

With Regards to Claim 20, Benaloh discloses an apparatus for tracing content in a highly distributed system, comprising:

a) means for receiving at the apparatus content associated with a content owner; (see Benaloh (see Benaloh col. 1, lines 63-66: content received; col. 12, lines 10-

14: network (distributed) access to content); col. 4, lines 18-20; col. 4, lines 32-37: software, implementation means)

b) decryption means for decrypting the received content by the apparatus; (see Benaloh col. 10, lines 16-19: decrypt content; col. 4, lines 18-20; col. 4, lines 32-37: software, implementation means)

c) means for determining an identifier that uniquely identifies the apparatus that received the content and has decrypted the content; (see Benaloh col. 6, lines 25-27: serial number, identifier for content player; col. 4, lines 32-37: software, implementation means)

d) means for modifying the decrypted content by the apparatus by embedding at least one of a fingerprint or watermark generated from the unique identifier into the decrypted content; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint; col. 4, lines 32-37: software, implementation means)

e) means for wrapping the modified content; (see Benaloh col. 8, lines 49-50; col. 11, lines 55-62; col. 9, lines 8-11: watermark, fingerprint; col. 4, lines 32-37: software, implementation means)

f) means for determining a set of information associated with the decryption of the content; (see Benaloh col. 2, lines 36-39; col. 1, line 54-58: identify (trace) entity that decrypted content; col. 4, lines 18-20; col. 4, lines 32-37: software, implementation means)

Benaloh discloses means for implementation. (see Benaloh col. 4, lines 18-20; col.

4, lines 32-37: software, implementation means) Benaloh does not specifically disclose providing the set of information associated with the decrypted content to the content owner

However, Cooper discloses:

g) providing the set of information to the content owner. (see Cooper paragraph [0071], lines 1-4; paragraph [0298], lines 1-3: report unauthorized content usage)

It would have been obvious to one of ordinary skill in the art to modify Benaloh for providing the second set of information to the content owner as taught by Cooper. One of ordinary skill in the art would have been motivated to employ the teachings of Cooper in order to enable the capability to mark content files with an authenticated digital signature that uniquely identifies the source. (see Cooper paragraph [0017], lines 7-13)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carlton V. Johnson whose telephone number is 571-270-1032. The examiner can normally be reached on Monday thru Friday , 8:00 - 5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Carlton V. Johnson
Examiner
Art Unit 2136

CVJ
May 27, 2008

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136